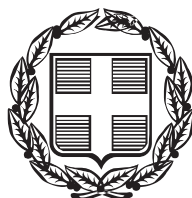


ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΔΕΥΤΕΡΟ **Αρ. Φύλλου 3320**

27 Δεκεμβρίου 2013

ΑΠΟΦΑΣΕΙΣ

Αριθμ. ΥΑΠ/Φ.60/3431

Τροποποίηση Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) ο οποίος κυρώθηκε με την υπ' αριθ. ΥΑΠ/Φ.60/38/232 κοινή απόφαση του Υπουργού Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και του Υφυπουργού Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)» (ΦΕΚ 799/Β΄/9-6-2010).

ΟΙ ΥΦΥΠΟΥΡΓΟΙ ΔΙΟΙΚΗΤΙΚΗΣ ΜΕΤΑΡΡΥΘΜΙΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ - ΥΠΟΔΟΜΩΝ, ΜΕΤΑΦΟΡΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Έχοντας υπόψη:

1. Τις διατάξεις του άρθρου 20 του Ν. 3448/2006 «Για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα και τη ρύθμιση θεμάτων αρμοδιότητας Υπουργ/15.3.2003), όπως ισχύουν

2. Τις διατάξεις του άρθρου 25 του Ν. 3536/2007 «Ειδικές ρυθμίσεις μεταναστευτικής πολιτικής και λοιπών ζητημάτων αρμοδιότητας Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης», (ΦΕΚ42 Α΄/23.2.2007),

3. Το Π.Δ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές» (ΦΕΚ 125/Α΄),

4. Την απόφαση της ΕΕΤΤ 248/71/2002 «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β'),

5. Την υπ' αριθ. 696/108/11-7-2013 Απόφαση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων «Παροχή σύμφωνης γνώμης επί του σχεδίου τροποποίησης του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)»,

6. Την υπ' αριθμ. οικ. 329/3-7-2013 απόφαση με θέμα: «Καθορισμός αρμοδιοτήτων Υφυπουργού Υποδομών, Μεταφορών και Δικτύων Μιχαήλ Παπαδόπουλου (ΦΕΚ Β΄1655/4-7-2013), όπως τροποποιήθηκε με την αρ. 1208/10-7-2013 όμοια της «Τροποποίηση ανάθεσης αρμοδιοτήτων στον Υφυπουργό Υποδομών, Μεταφορών και Δικτύων» Μιχαήλ Παπαδόπουλου (ΦΕΚ 1718/12-7-2013).

7. Την υπ' αριθμ. 2303/2-7-2013 απόφαση του Πρωθυπουργού και Υπουργού Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης «Ανάθεση αρμοδιοτήτων στην Υφυπουργό Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης, Παρασκευή Χριστοφιλοπούλου» (ΦΕΚ 1632/Β΄).

8. Το γεγονός ότι από την απόφαση αυτή δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού, αποφασίζουμε:

Άρθρο 1

Τροποποιούμε τον Κανονισμό Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), ο οποίος κυρώθηκε με την υπ' αριθ. ΥΑΠ/Φ.60/38/232/28-5-2010 κοινή απόφαση του Υπουργού Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και του Υφυπουργού Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)» (ΦΕΚ 799/Β΄/9-6-2010) ως ακολούθως:

1) Το άρθρο 1 της υπ' αριθ. ΥΑΠ/Φ.60/38/232/28-5-2010 της κοινής Υπουργικής απόφασης (ΦΕΚ 799/Β΄/9-6-2010) τροποποιείται ως εξής :

«ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ ΥΠΟΥΡΓΕΙΟ ΔΙΟΙΚΗΤΙΚΗΣ ΜΕΤΑΡΡΥΘΜΙΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΥΠΗΡΕΣΙΑ ΑΝΑΠΤΥΞΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ http://www.yap.gov.gr»

2) Η παράγραφος 1.2.1.7 του άρθρου 1 αντικαθίσταται ως εξής :

«1.2.1.7 Πολιτική Πιστοποιητικού 7 (ΠΠ 7)

Η Πολιτική Πιστοποίησης 7 (ΠΠ 7) αναφέρεται σε Πιστοποιητικά Φορέων του δημοσίου τομέα ή ανεξάρτητων διοικητικών αρχών ή ΝΠΙΔ, τα οποία χρησιμοποιούνται για ψηφιακή υπογραφή (προηγμένη ηλεκτρονική υπογραφή) και κρυπτογράφηση ηλεκτρονικών μηνυμάτων και εγγράφων που εκδίδονται από τους εν λόγω Φορείς.

Για τα Πιστοποιητικά αυτά «Τελικό Χρήστη» αποτελεί ο ίδιος ο Φορέας, στο όνομα του οποίου εκδίδεται το Πιστοποιητικό, ενώ ο εκάστοτε νόμιμος εκπρόσωπος του Φορέα, ή ο νόμιμος εκπρόσωπος του εποπτεύοντος Φορέα, ή άλλο νομίμως εξουσιοδοτημένο για αυτό το σκοπό φυσικό πρόσωπο (εφεξής «Εκπρόσωπος του Φορέα») είναι υπεύθυνος για τη διαχείριση του ως άνω Πιστοποιητικού ως «αιτών» το πιστοποιητικό (Subscriber). Τα Πιστοποιητικά αυτά δύνανται να δημιουργούνται ή/και να αποθηκεύονται σε ΑΔΔΥ ή σε άλλη Ασφαλή Κρυπτογραφική Μονάδα. Η όποια αναφορά σε «Εκπρόσωπο Φορέα» σε αυτό το έγγραφο, αφορά τη συγκεκριμένη Πολιτική Πιστοποίησης και μόνο».

3) Ο πίνακας 8, με τίτλο « Βασικά Πεδία Προφίλ Πιστοποιητικού», του άρθρου 1, αντικαθίσταται ως εξής:

«Πίνακας 8 : Βασικά πεδία προφίλ Πιστοποιητικού»

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Εκδοση)	Βλ. ΠΠ §7.1.1
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)

Signature Algorithm (Αλγόριθμος Υπογραφής)	Ο αλγόριθμος που χρησιμοποιήθηκε για την υπογραφή του Πιστοποιητικού (Βλ. §7.1.3 της ΠΠ)
Issuer DN (Διακριτικό Όνομα Εκδότη)	Βλ. §7.1.4 της ΠΠ
Valid From (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280.
Valid To (Ισχύει Μέχρι)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280. Η περίοδος ισχύος θα καθορίζεται σύμφωνα με τους περιορισμούς που ορίζει η §6.3.2 της ΠΠ.
Subject DN (Διακριτικό Όνομα Υποκειμένου)	Βλ. §7.1.4 της ΠΠ
Subject Public Key (Δημόσιο Κλειδί Υποκειμένου)	Κωδικοποιημένο σύμφωνα με το RFC 5280 με τη χρήση αλγορίθμων που προσδιορίζονται στην §7.1.3 της ΠΠ και με μήκη κλειδιών που προσδιορίζονται στην §6.1.5 της ΠΠ.
Signature (Υπογραφή)	Παράγεται και κωδικοποιείται σύμφωνα με το RFC 5280

4) Η παράγραφος 7.1.1 του άρθρου 1 αντικαθίσταται ως εξής:

«7.1.1 Αριθμός (-οί) έκδοσης

Τα Πιστοποιητικά των εκδοτριών ΑΠ και Τελικών Χρηστών αποτελούν Πιστοποιητικά Χ.509 Έκδοσης 3 και το πεδίο έκδοσης τους (version) θα έχει την τιμή V3 (2) σύμφωνα με το RFC 5280».

5) Μετά το Παράρτημα Α του άρθρου 1 προστίθεται παράρτημα Β ως εξής :

«ΠΑΡΑΡΤΗΜΑ Β΄ - Πολιτική/ Δήλωση Πρακτικής Χρονοσήμανσης της ΑΠΕΔ

Σύμφωνα με τις διατάξεις της υπ' αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β΄/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)», καθορίζονται οι όροι, οι προϋποθέσεις και οι διαδικασίες για την παροχή υπηρεσιών πιστοποίησης από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), σύμφωνα με τις διατάξεις του άρθρου 20 του Ν3448/2006 (ΦΕΚ 57/Α΄/2006). Εξάλλου, με την υπουργική απόφαση ΥΑΠ/Φ.60/76/984/9-4-2012 (ΦΕΚ 1162/Β΄/2012) καθορίστηκαν οι οργανικές μονάδες για την παροχή υπηρεσιών πιστοποίησης της ΑΠΕΔ.

Με την Υπουργική Απόφαση ΥΑΠ/Φ.40.4/163 (ΦΕΚ 401/Β΄/22-02-2013) καθορίζονται οι διαδικασίες και ο τρόπος ηλεκτρονικής επιβεβαίωσης της λήψης εγγράφων και της ασφαλούς χρονοσήμανσης, οι προδιαγραφές και τα πρότυπα του συστήματος για τη γνωστοποίηση εγγράφων σε φυσικά πρόσωπα ή Ν.Π.Ι.Δ. με χρήση ΤΠΕ και η ηλεκτρονική διακίνηση εγγράφων μεταξύ φορέων του δημόσιου τομέα και των φυσικών προσώπων ή ΝΠΙΔ.

Η ΑΠΕΔ παρέχει υπηρεσίες χρονοσήμανσης με σκοπό τη δημιουργία των απαραίτητων τεκμηρίων για την ύπαρξη ενός συνόλου ψηφιακών δεδομένων σε μία συγκεκριμένη χρονική στιγμή. Η Πολιτική Χρονοσήμανσης και η Δήλωση Πρακτικής Χρονοσήμανσης της ΑΠΕΔ έχουν συγχωνευτεί σε ένα ενιαίο παράρτημα με την ονομασία Πολιτική/ Δήλωση Πρακτικής Χρονοσήμανσης (ΠΔΠΧ). Με τις διατάξεις του παρόντος παραρτήματος καθορίζονται οι πολιτικές και πρακτικές που εφαρμόζονται για την παροχή υπηρεσιών χρονοσήμανσης από την ΑΠΕΔ, ως Πάροχος Υπηρεσιών Χρονοσήμανσης (ΠΥΧ). Η παρούσα ΠΔΠΧ αποσκοπεί στον καθορισμό των σχετικών διαδικασιών της ΑΠΕΔ ως ΠΥΧ.

Η ΑΠΕΔ εφαρμόζει ένα έμπιστο και αξιόπιστο σύστημα ακριβούς χρόνου για την παροχή υπηρεσιών χρονοσήμανσης με χρήση της Υποδομής Δημόσιου Κλειδιού σύμφωνα με τις διατάξεις της κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων (ΦΕΚ 799/Β΄/09-06-2010) και του προηγουμένου παραρτήματος της παρούσας. Η ΑΠΕΔ λαμβάνει όλα τα αναγκαία μέτρα για τη διασφάλιση της εμπιστευτικότητας και τη διατήρηση της ακεραιότητας των ιδιωτικών κρυπτογραφικών κλειδιών ως ΠΥΧ.

1. Ορισμοί:

- Χρονοσήμανση: Αλληλουχία χαρακτήρων ή στοιχεία που δηλώνουν με ασφάλεια την ημερομηνία και ώρα που έχει λάβει χώρα μία πράξη ή ενέργεια και εκδίδεται από πάροχο υπηρεσιών χρονοσήμανσης.
- Υπηρεσία χρονοσήμανσης: Η δημιουργία των απαραίτητων τεκμηρίων για ένα σύνολο δεδομένων σε ψηφιακή μορφή, έτσι ώστε να μπορεί να αποδειχθεί ότι τα δεδομένα αυτά υπήρχαν σε μία συγκεκριμένη χρονική στιγμή.
- Πάροχος Υπηρεσιών Χρονοσήμανσης: Ο φορέας που εκδίδει χρονοσημάνσεις κατ' εφαρμογή του θεσμικού πλαισίου διαπίστευσης της ΕΕΤΤ και περιλαμβάνεται στον κατάλογο εμπίστευσης της ΕΕΤΤ (Κατάλογος Εμπίστευσης εποπτευόμενων/ διαπιστευμένων Παροχών Υπηρεσιών Πιστοποίησης - TSL).
- Ακριβής χρόνος: Η αναφορά στοιχείων με τα οποία προσδιορίζεται το έτος, ο μήνας, η ημερομηνία, η ώρα, τα λεπτά και τα δευτερόλεπτα. Για τους φορείς του Δημόσιου Τομέα, σύμφωνα με τις διατάξεις της παρούσας, ο ακριβής χρόνος προσδιορίζεται με βάση την Εθνική ώρα Ελλάδας.
- Ηλεκτρονικό έγγραφο: Κάθε μέσο, το οποίο χρησιμοποιείται από υπολογιστικό - πληροφοριακό σύστημα, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων που δεν μπορούν να αναγνωστούν άμεσα, όπως και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό, στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφόσον το εν λόγω περιεχόμενο επιφέρει έννομες συνέπειες ή προορίζεται ή είναι πρόσφορο να αποδείξει γεγονότα που μπορούν να έχουν έννομες συνέπειες.
- Μεταφόρτωση ηλεκτρονικού εγγράφου: Η μεταφορά του συνόλου του περιεχομένου ενός ηλεκτρονικού εγγράφου από το διαδικτυακό τόπο στον οποίο αυτό έχει αναρτηθεί σε αποθηκευτικό χώρο της επιλογής του παραλήπτη.
- Συντονισμένος Παγκόσμιος Χρόνος (Coordinated Universal Time -UTC): Χρονική κλίμακα με βάση το δευτερόλεπτο όπως ορίζεται στη σύσταση ITU-R TF.460-5.
- UTC(x): Ο Συντονισμένος Παγκόσμιος Χρόνος που παράγεται από το εργαστήριο χ.

2. Πολιτική Χρονοσήμανσης:

Η Πολιτική Χρονοσήμανσης είναι ένα σύνολο κανόνων που αφορά την έκδοση και διαχείριση των χρονοσημάνσεων που παράγονται από την ΑΠΕΔ ως ΠΥΧ για τους τελικούς χρήστες. Οι υπηρεσίες χρονοσήμανσης περιλαμβάνουν την οργάνωση της υποδομής και την έκδοση

χρονοσημάνσεων. Οι συγκεκριμένες υπηρεσίες παρέχονται από την ΑΠΕΔ στους τελικούς χρήστες στο πλαίσιο λειτουργίας της υποδομής δημοσίου κλειδιού της ΑΠΕΔ. Οι υπηρεσίες παρέχονται κυρίως για την υποστήριξη ψηφιακών υπογραφών αλλά και για οποιαδήποτε εφαρμογή απαιτεί αποδεικτικά στοιχεία για την ύπαρξη κάποιων δεδομένων μία συγκεκριμένη χρονική στιγμή. Η ΑΠΕΔ διασφαλίζει την χρήση αξιόπιστης πηγής ώρας και την κατάλληλη διαχείριση των συστημάτων χρονοσήμανσης. Ειδικότερα, οι υπηρεσίες χρονοσήμανσης περιλαμβάνουν:

- Λειτουργία αντιστοίχισης υπηρεσίας χρονοσήμανσης: Η υπηρεσία χρονοσήμανσης αντιστοιχίζει ένα ηλεκτρονικό αρχείο με μια συγκεκριμένη χρονική στιγμή και εγγυάται την ακρίβεια της χρονικής στιγμής και της αντιστοίχισης.
- Ανάκτηση ακριβούς χρόνου: Η διαδικασία χρονοσήμανσης χρησιμοποιεί τον επίσημο χρόνο Coordinated Universal Time (UTC), μέσα από τέτοιες πηγές χρόνου που παρέχουν ασφαλή και ιχνηλάσιμα κανάλια επικοινωνίας. Η μέγιστη απόκλιση από το ρολόι της πηγής είναι ένα (1) δευτερόλεπτο. Η παρεχόμενη προς τους τελικούς χρήστες χρονοσήμανση περιλαμβάνει την απαραίτητη προσαύξηση κατά 2 ώρες έτσι ώστε να είναι σύμφωνα με τη χρονική ζώνη της Ελλάδας.
- Παραγωγή χρονοσημάνσεων: Το σύστημα παράγει χρονοσημάνσεις σύμφωνα με την τεχνική προδιαγραφή ETSI TS 102 023 V1.2.2 (2008-10) "Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities" και το RFC 3628 για τις απαιτήσεις που πρέπει να πληρούν οι ΠΥΧ, καθώς και με την τεχνική προδιαγραφή ETSI TS 101 861 V1.4.1 (2011-07) "Electronic Signatures and Infrastructures (ESI), Time stamping profile" και το RFC 3161 για την έκδοση και τη λήψη ασφαλών χρονοσημάνσεων.
- Επαλήθευση υπογραφών και πιστοποιητικών χρονοσήμανσης: Το κλειδί επαλήθευσης της ψηφιακά υπογεγραμμένης χρονοσήμανσης παρέχεται μέσω ψηφιακού πιστοποιητικού. Τα πιστοποιητικά των συστημάτων της χρονοσήμανσης είναι δημοσιευμένα από την ΑΠΕΔ στον σχετικό κατάλογο της ΥΔΚ της ΑΠΕΔ (https://pki.ermis.gov.gr/repositoryhtml) και η εγκυρότητα τους μπορεί να επαληθευτεί σε σχέση με την παραχθείσα χρονοσήμανση του ηλεκτρονικού εγγράφου.
- Πιστοποιητικό ΠΥΧ: Το πιστοποιητικό παράγεται σύμφωνα με το πρότυπο X.509 v3.

Οι χρονοσφραγίδες παράγονται από την ΑΠΕΔ μέσω του παρακάτω συνδέσμου. TSA uri: http://timestamp.ermis.gov.gr/TSS/HttpTspServer

Προσδιοριστής Αντικειμένου - OID Policy: 1.3.6.1.4.1.601.10.3.1

Το προφίλ των βασικών πεδίων του πιστοποιητικού χρονοσήμανσης της ΑΠΕΔ περιγράφονται στον Πίνακα 1.

Πίνακας 1. Προφίλ των Βασικών Πεδίων του Πιστοποιητικού Χρονοσήμανσης

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Εκδοση)	V3
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)
Signature Algorithm (Αλγόριθμος Υπογραφής)	SHA1 RSA
Issuer DN (Διακριτικό Όνομα Εκδότη)	cn=HPARCA Time Stamping Services ou=HPARCA o=Hellenic Public Administration Certification Services c=GR
Valid From (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280.
Valid To (Ισχύει Μέχρι)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280. Η περίοδος ισχύος δεν υπερβαίνει τη διάρκεια ισχύος του πιστοποιητικού της Πρωτεύουσας Αρχής Πιστοποίησης.
Subject DN (Διακριτικό Όνομα Υποκειμένου)	cn=HPARCA Time Stamping Services ou=HPARCA o=Hellenic Public Administration Certification Services c=GR
Μέγεθος Κλειδιού	2048 bits
Χρήση κλειδιού	Ψηφιακή υπογραφή, Κρυπτογράφηση κλειδιού
Βελτιωμένη χρήση κλειδιού	Χρονική σήμανση

Η υπηρεσία χρονοσήμανσης παρέχεται σύμφωνα με τις διατάξεις της υπ' αριθ. πρωτ.: ΥΑΠ/Φ.40.4/163 «Ρυθμίσεις για α) τη διαδικασία και τον τρόπο ηλεκτρονικής επιβεβαίωσης της λήψης και της ασφαλούς χρονοσήμανσης, β) τις προδιαγραφές και τα πρότυπα του συστήματος για τη γνωστοποίηση εγγράφων σε φυσικά πρόσωπα ή Ν.Π.Ι.Δ. με χρήση ΤΠΕ και γ) την ηλεκτρονική διακίνηση εγγράφων μεταξύ φορέων του δημόσιου τομέα και των φυσικών προσώπων ή ΝΠΙΔ» (ΦΕΚ 401/Β΄/22-02-2013).

3. Υποχρεώσεις

Η ΑΠΕΔ εγγυάται και διασφαλίζει την εφαρμογή της Πολιτικής Χρονοσήμανσης σύμφωνα με τις διατάξεις της παραγράφου 2 του παραρτήματος Β΄ της παρούσας, καθώς και των απαιτήσεων της παραγράφου 4 του παραρτήματος Β΄ «Δήλωση Πρακτικής».

Ειδικότερα, ως προς τους τελικούς χρήστες και τους τρίτους συμμετέχοντες η ΑΠΕΔ διασφαλίζει ότι η μέγιστη απόκλιση από το UTC ρολόι της πηγής είναι ένα (1) δευτερόλεπτο.

Οι τελικοί χρήστες και οι τρίτοι συμμετέχοντες οφείλουν να επαληθεύουν την εγκυρότητα και την ορθότητα της χρονοσήμανσης.

4. Δήλωση Πρακτικής

Η Δήλωση Πρακτικής της ΑΠΕΔ περιγράφει τον τρόπο με τον οποίο υλοποιείται η Πολιτική Χρονοσήμανσης, η διαδικασία για τη δημιουργία της Υπηρεσίας Χρονοσήμανσης και η διατήρησης της ακρίβειας του ρολογιού.

Για την υλοποίηση της Υπηρεσίας Χρονοσήμανσης εφαρμόζεται το πρωτόκολλο Time-Stamp Protocol (IETF RFC 3161) και ο Εθνικός Χρόνος UTC (ΕΙΜ), που παράγεται στο Εργαστήριο Χρόνου και Συχνότητας του Ελληνικού Ινστιτούτου Μετρολογίας (ΕΙΜ), το οποίο αναγνωρίζεται διεθνώς ως ένας αξιόπιστος φορέας στη μέτρηση και τήρηση του χρόνου. Το ΕΙΜ διαθέτει μια υψηλής τεχνολογίας και ακρίβειας συστοιχία πρότυπων ατομικών ρολογιών, που μπορεί να παράγει και να τηρήσει τον εθνικό χρόνο με μεγάλη αξιοπιστία.

Το Εργαστήριο Χρόνου - Συχνότητας υλοποιεί μέσω κβαντικών φαινομένων τις μονάδες του Χρόνου (s) και της Συχνότητας (Hz) με την χρήση τριών πρωτευόντων ατομικών προτύπων-ρολογιών καισίου. Η ακρίβεια τήρησης του χρόνου UTC είναι 1 ns.

Το χρονικό διάστημα για το οποίο διατηρείται όλη η σχετική πληροφορία σχετικά με την λειτουργία χρονοσήμανσης είναι τα δέκα χρόνια. Οι αποδεκτοί Time Stamp Hashes είναι οι:

SHA-1, SHA-256, SHA-384, SHA-512.

4.1. Πιστοποιητικά συστημάτων χρονοσήμανσης

Τα κρυπτογραφικά κλειδιά και τα πιστοποιητικά των εξυπηρετητών χρονοσήμανσης (TimeStamping Server) παράγονται, αποθηκεύονται και χρησιμοποιούνται μέσα σε ασφαλείς κρυπτογραφικές μονάδες της ΑΠΕΔ οι οποίες πληρούν τις προϋποθέσεις και τις απαιτήσεις της απόφασης της ΕΕΤΤ 295/64 «Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων» (ΦΕΚ 1730/Β΄/24-11-2003).

Τα Πιστοποιητικά των Εξυπηρετητών Χρονοσήμανσης (TimeStamping Server) δημοσιεύονται στον σχετικό κατάλογο της ΥΔΚ της ΑΠΕΔ (https://pki.ermis.gov.gr/repositoryhtml).

4.2. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

Η ΑΠΕΔ, ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), υπογράφει τα Πιστοποιητικά των Εξυπηρετητών Χρονοσήμανσης. Το Πιστοποιητικό της ΑΠΕΔ, καθώς και τα Πιστοποιητικά των Εξυπηρετητών Χρονοσήμανσης είναι διαθέσιμα στους Τρίτους Συμμετέχοντες, διαδικτυακά μέσω των χώρων αποθήκευσης της ΑΠΕΔ, καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού η οποία ενσωματώνεται στο Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης.

Οι Όροι Τρίτου Συμμετέχοντα απαιτούν από τους τελευταίους τη διαβεβαίωση ότι διαθέτουν επαρκείς πληροφορίες για να αποφασίσουν σε ποιο βαθμό θα βασιστούν στις πληροφορίες που αναγράφονται στο Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης, ότι είναι αποκλειστικά υπεύθυνοι για το εάν θα βασιστούν ή όχι στις πληροφορίες αυτές και ότι θα υποστούν τις νόμιμες συνέπειες από την αποτυχία τους να εκπληρώσουν τις υποχρεώσεις του Τρίτου Συμμετέχοντα σύμφωνα με την παρούσα Πολιτική/Δήλωση Πρακτικής Χρονοσήμανσης της ΑΠΕΔ.

Οι Τρίτοι Συμμετέχοντες αποδέχονται τους Όρους Τρίτου Συμμετέχοντα ως προϋπόθεση για να εμπιστευθούν το Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης. Η εξάρτηση από Πιστοποιητικό πρέπει να είναι εύλογη σύμφωνα με τις περιστάσεις. Η ΑΠΕΔ και οι εκδότριες ΑΠ δε φέρουν ευθύνη για την αξιολόγηση της καταλληλότητας χρήσης των Πιστοποιητικών Εξυπηρετητών Χρονοσήμανσης.

Η επαναδημιουργία κλειδιών των Πιστοποιητικών Εξυπηρετητών Χρονοσήμανσης γίνεται κάτω από αυστηρά μέτρα ελέγχου, σε ειδικές Τελετές Δημιουργίας Κλειδιών σύμφωνα με την §6.1.1 της Πολιτικής Πιστοποιητικών. Πιστοποίηση νέου κλειδιού μπορεί να αιτηθεί μόνο ο Εκπρόσωπος της ΑΠΕΔ. Η ΑΠΕΔ έχει δικαίωμα να ζητήσει την ανάκληση πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης. Η ΑΠΕΔ ανακαλεί Πιστοποιητικά Εξυπηρετητών Χρονοσήμανσης, εφόσον:

- Ανακαλύψει ή έχει λόγο να πιστεύει ότι έχει υπάρξει έκθεση σε κίνδυνο του ιδιωτικού κλειδιού Πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης.
- Ανακαλύψει ή έχει λόγο να πιστεύει ότι το Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από την παρούσα Πολιτική.
- Διαπιστώσει ότι δεν τηρούνται οι όροι της παρούσας Πολιτικής ή υπάρχει παραίτηση από μια ουσιώδη προϋπόθεση για την Έκδοση Πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης.
- Η ΑΠΕΔ παύσει να λειτουργεί ως ΑΠ.

Σε περίπτωση ανάκλησης του Πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης εφαρμόζονται οι διατάξεις της παραγράφου 5 του κεφαλαίου Α της υπ' αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β΄/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.3. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας Προσωπικού

Σύμφωνα με τις διατάξεις της παραγράφου 5 του κεφαλαίου Α της υπ' αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β΄/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.4. Τεχνικά Μέτρα Ασφάλειας

Σύμφωνα με τις διατάξεις της παραγράφου 6 του κεφαλαίου Α της υπ' αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β΄/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.5. Έλεγχος Συμμόρφωσης και Άλλες Αξιολογήσεις

Σύμφωνα με τις διατάξεις της παραγράφου 8 του κεφαλαίου Α της υπ' αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β΄/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.6. Άλλα Επιχειρησιακά και Νομικά Ζητήματα

Σύμφωνα με τις διατάξεις της παραγράφου 9 του κεφαλαίου Α της υπ' αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β΄/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.7. Τοποθεσίες δημοσίευσης

Όλα τα δημόσια έγγραφα που αφορούν την ΑΠΕΔ ως ΠΥΧ, είναι διαθέσιμα στην επίσημη ιστοσελίδα της Υπηρεσίας Ανάπτυξης Πληροφορικής του ΥΔΜΗΔ http://www.yap.qov.gr όπως και στην ιστοσελίδα https://pki.ermis.gov.gr/repository.html. Η ΑΠΕΔ είναι υπεύθυνη για την τήρηση, ανανέωση και δημοσίευση όλων των παραπάνω στοιχείων.».

Άρθρο 2
Έναρξη ισχύος

Κατά τα λοιπά ισχύει η υπ' αριθ. ΥΑΠ/Φ.60/38/232 κοινή απόφαση του Υπουργού Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και του Υφυπουργού Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου» (ΦΕΚ 799/Β΄/9-6-2010).

Η ισχύς της παρούσας απόφασης αρχίζει από τη δημοσίευση της στην Εφημερίδα της Κυβερνήσεως.

Η απόφαση αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Αθήνα, 18 Δεκεμβρίου 2013

ΟΙ ΥΦΥΠΟΥΡΓΟΙ

ΔΙΟΙΚΗΤΙΚΗΣ ΜΕΤΑΡΡΥΘΜΙΣΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ	ΥΠΟΔΟΜΩΝ, ΜΕΤΑΦΟΡΩΝ ΚΑΙ ΔΙΚΤΥΩΝ
ΠΑΡΑΣΚΕΥΗ ΧΡΙΣΤΟΦΙΛΟΠΟΥΛΟΥ	**ΜΙΧΑΗΛ ΠΑΠΑΔΟΠΟΥΛΟΣ**



ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
ΚΑΠΟΔΙΣΤΡΙΟΥ 34 * ΑΘΗΝΑ 104 32 * ΤΗΛ. 210 52 79 000 * FAX 210 52 21 004